

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Accounts  
[REDACTED] and

Maintained at Premises Controlled by  
Google, LLC, USAO Reference No.  
[REDACTED]

20 MAG 02240

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Google, LLC ("Provider")

Federal Bureau of Investigation and United States Attorney's Office for the Southern  
District of New York

**1. Warrant.** Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau  
of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C.  
§ 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal  
Procedure 41, the Court hereby finds there is probable cause to believe the email accounts  
[REDACTED] and [REDACTED], maintained at premises  
controlled by Google, LLC, contain evidence, fruits, and instrumentalities of crime, all as specified  
in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the  
Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records  
specified in Section II of Attachment A hereto, for subsequent review by law enforcement  
personnel as authorized in Section III of Attachment A. The Government is required to serve a  
copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant  
and Order may be served via electronic transmission or any other means through which the  
Provider is capable of accepting service.

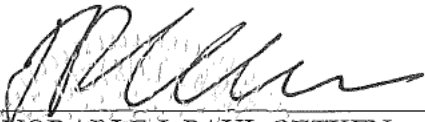
**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, and/or tamping with potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person, including but not limited to a representative of the enterprise domain, for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

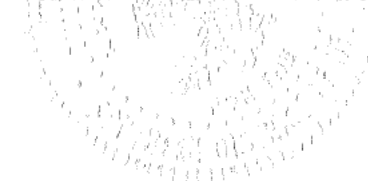
**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

\_\_\_\_\_  
Date Issued

\_\_\_\_\_  
Time Issued

  
\_\_\_\_\_  
HONORABLE J. PAUL OETKEN  
United States District Judge  
Southern District of New York



## **Email Search Attachment A**

### **I. Subject Accounts and Execution of Warrant**

This warrant is directed to Google, LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts [REDACTED] and [REDACTED] (the "Subject Accounts"). The Provider is directed to produce the information described below associated with the Subject Accounts, limited to content created, sent, or received on or after the date the accounts were created, through September 1, 2013.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts (subject to the time period limitation set forth above):

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Google Drive Content.* All Google Drive records associated with the Subject Accounts, including all documents and other records stored on the Google Drive accounts.

f. *Google Docs.* All Google Docs records associated with the Subject Accounts, including all documents created or stored in Google Docs.

g. *Google Calendar.* All calendar entries and records associated with the Subject Accounts.

h. *Location History.* All location records associated with the Subject Accounts.

i. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Accounts, including specifically by Cookie, email account, phone number, Google Account ID, Android ID, or other account or device identifier.

j. *Device Information.* Any information identifying the device or devices used to access the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber

Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the Subject Accounts;

k. *Android Services*. All records relating to Android services associated with the Subject Accounts.

l. *Preserved or backup records*. Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the “Subject Offenses”), including the following:

a. Evidence relating to, including communications with, any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee’s plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee’s actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to false and fraudulent representations made to potential or actual investors, including drafts of any corporate documents and related materials;

e. Evidence relating to Fraud Guarantee’s members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

f. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

g. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

h. Evidence of meetings between Parnas, Correia, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

i. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

j. Passwords or other information needed to access user's online accounts.